(19) Europäisches Patentamt
European Patent Office
Office europ´en des brevets

(11) Publication number: **0 510 433 A2**

(12) EUROPEAN PATENT APPLICATION

(21) Application number: 92106105.7

(51) Int. Cl.5: **H01L 25/18**, H01L 23/58

(22) Date of filing: 09.04.92

(30) Priority: 26.04.91 US 692334

(43) Date of publication of application:
28.10.92 Bulletin 92/44

(84) Designated Contracting States:
FR GB

(71) Applicant: Hughes Aircraft Company
7200 Hughes Terrace P.O. Box 45066
Los Angeles, California 90045-0066(US)

(72) Inventor: Thiele, Alan G.
3444 Lady Hill Road
San Diego, California 92130(US)
Inventor: Williams, Ronald L.
1421 Pine Heights Way
San Marcos, California 92069(US)

(74) Representative: Witte, Alexander, Dr.-Ing. et al
Augustenstrasse 7
W-7000 Stuttgart 1(DE)

(54) Secure circuit structure.

(57) A secure circuit structure includes a pair of opposed substrates (2, 4) having a volatile circuit (6a, 6b) fabricated on at least one, and perferably both substrates (2, 4). A maintenance circuit (12-26, A-E) for the volatile circuit (6a, 6b) extends between the substrates (2, 4) so that it is interrupted, thereby altering the volatile circuit (6a, 6b) and rendering reverse engineering attempts futile, if the substrates (2, 4) are moved with respect to each other by opening the circuit package. The maintenance circuit (12-26, A-E) preferably includes a series of mating conductive indium bumps (12, 14, A-E) that extend from the opposed substrates (2, 4) and mechanically bond the substrates (2, 4) together. The secured volatile circuit (6a, 6b) may be a random access memory storing an access code, maintained by a battery power supply circuit.

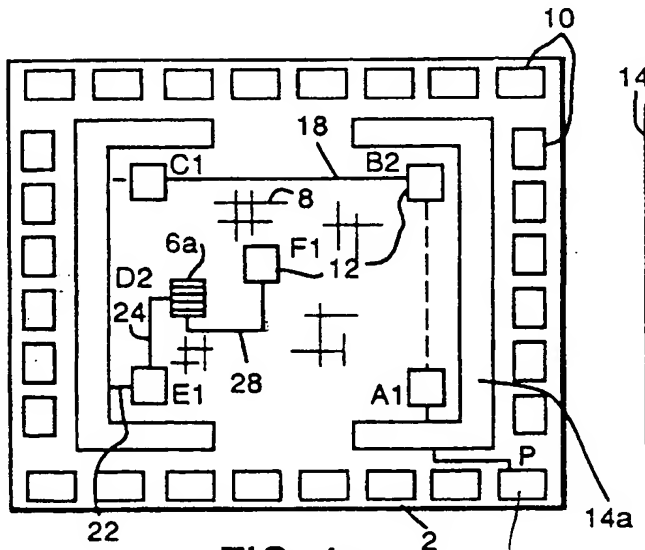

FIG. 1a.

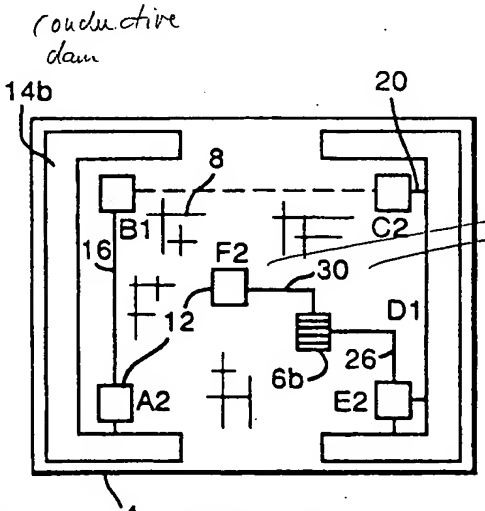

FIG. 1b.

EP 0 510 433 A2

BACKGROUND OF THE INVENTION

Field of the Invention

This invention relates to the protection of electrical circuitry from reverse engineering, and more particularly to the protection of access codes embedded within integrated circuitry.

Description of the Related Art

It is very important to prevent unauthorized access to certain portions of electrical circuits, particularly integrated circuits. For example, digital codes or other data may be stored in certain portions of the circuit to prevent its unauthorized use; the circuit will function properly only if the user enters the appropriate code. Such circuitry may be compromised, however, by various methods of analysis, such as visual inspection, microprobing, secondary electron emission voltage-contrast analysis, etc. A number of techniques have been used in the past to prevent such reverse engineering.

Perhaps the most basic technique is to enclose the circuit in plastic encapsulation or protective die coating. However, access to the circuitry can be gained by mechanical or acid drilling through the encapsulation material. Another approach is to add misleading circuit topology so as to disguise the portion of the circuitry to be protected, or to customize each different die with its own specific code. An example of this approach is disclosed in U.S. Patent No. 4,766,516, "Method and Apparatus for Securing Integrated Circuits from Unauthorized Copying and Use," August 23, 1988, to Ozdemir et al. and assigned to Hughes Aircraft Company. These techniques may retard, but generally do not totally prevent, successful reverse engineering. Patent No. 4,766,516 also discloses a use control scheme for a secure system which has circuitry on several printed circuit boards. Each circuit transmits a control code to enable the circuitry on the next board in order when it itself has received its control code; an external software verification unit transmits the control code for the first board. Overall system operation is disabled if any of the boards are tampered with or missing.

Other methods include changing the circuit chip at regular intervals, and encapsulating the chip with wires that easily break if an attempt is made to open the encapsulation and probe the chip. Such methods are discussed in W. Diffie and M. E. Hellman, "Privacy and Authentication: An Introduction to Cryptography", Proc. IEEE, Vol. 67, No. 3, March 1979.

SUMMARY OF THE INVENTION

The present invention seeks to provide a circuit structure that is more secure than prior circuits, and disables itself when access is attempted so that it cannot be reverse engineered.

The circuit structure includes a pair of opposed substrates, with a volatile circuit fabricated on at least one of the substrates so that it faces the other substrate. The substrates are held in a fixed position with respect to each other, with the volatile circuit maintained by a maintenance circuit that extends between the substrates. Moving the substrates with respect to each other interrupts the maintenance circuit, thereby altering the volatile circuit so that it cannot be successfully reversed engineered.

In a preferred embodiment, the maintenance circuit includes several pairs of opposed conductive indium bumps that extend from the opposed substrates to contact each other and establish both a mechanical bond and an electrical path for the maintenance circuit. This circuit extends in multiple traverses back and forth between the substrates, through the bumps. The volatile circuit may be divided into portions located on each of the substrates, in which case the maintenance circuit can also interconnect the divided portions. Opposed peripheral dams may also be provided on the substrates to impede access to the interior of the circuit structure. The dams may be connected such that open circuiting a pair of opposed dams or short circuiting adjacent dams also interrupts the maintenance circuit.

The volatile circuit is preferably implemented as a volatile memory, with a power supply circuit for the memory serving as the maintenance circuit. Moving the substrates relative to each other breaks the power supply circuit, causing the memory information to erase in the case of a static memory, or to decay for a dynamic memory. In either case, a secure code originally written into the memory is altered so that reverse engineering the memory will not yield the original code.

These and other features and advantages of the invention will be apparent to those skilled in the art from the following detailed description, taken together with the accompanying drawings, in which:

BRIEF DESCRIPTION OF THE DRAWINGS

FIGs. 1a and 1b are plan views of the two substrates before they are joined together in the secure circuit structure;

FIG. 2 is a perspective view of the two substrates about to be joined together;

FIG. 3 is an elevation view of the circuit structure, with a maintenance circuit indicated in dashed lines;

FIG. 4 is a perspective view of the secure circuit

structure aligned for attachment to a circuit board; and

FIG. 5 is a sectional view of the circuit structure mounted on the circuit board.

DETAILED DESCRIPTION OF THE INVENTION

The present invention takes a direct departure from the prior approach of trying to protect a secure circuit by preventing physical access to the circuit. In the new approach described herein, it is conceded that someone who wishes to reverse engineer the secure circuit may gain physical access to it. However, it establishes a circuit structure that modifies the secure circuit in case such physical access is gained, thereby frustrating any attempts to reverse engineer the original circuit.

A somewhat simplified circuit structure that illustrates the principles of the invention is shown in FIGS. 1a and 1b. The circuit structure is formed from a pair of substrates 2 and 4, prepared from a suitable semiconductor material such as silicon. When assembled, substrate 4 is "flip-chip" mounted to substrate 2 as illustrated in FIG. 2, with the circuits on each substrate facing each other.

A circuit 6a to be secured is fabricated on substrate 2. The entire circuit may be formed on substrate 2, or it may be divided into two portions, with one portion 6a on substrate 2 and the other portion 6b on substrate 4.

The secure circuit is preferably implemented as a volatile digital memory, such as a static or dynamic RAM (random access memory). Dynamic RAM cells use a transistor and capacitor combination, with the digital information represented by a charge stored on each of the capacitors in the memory array. A static RAM, on the other hand, uses a series of transistors to form a flip-flop for each cell in the array. Both types of memory are considered "volatile" in the sense that they must be constantly maintained to retain their memory codes. The maintenance function is performed by a power supply. If a dynamic RAM is not replenished with a refresh signal (typically every two ms), as well as supplied with a power supply signal, the capacitors will lose their charge and the code will be altered. If power is removed from a static memory, the flip-flop will reset and the memory will display a different code when power is restored.

While a RAM using non-symmetrical transistor elements is used in the preferred embodiment of the invention, any other type of secure circuit that similarly requires the presence of a maintenance circuit to retain the original circuit configuration could be employed. The secure circuit 6a, 6b will generally be part of a larger overall circuit, indicated by hash lines 8.

Substrate 2 is larger than substrate 4, and includes a series of conductive contact pads 10 around its periphery for electrically communicating with a circuit board. At least one conductive "bump" 12, and preferably a plurality of such bumps, are formed on the opposed faces of the two substrates in alignment with each other. Substrate 4 is emplaced over substrate 2 so that the opposed conductive bumps on the two substrates mate with each other, providing electrical connections between the substrates and also a mechanical engagement that bonds the substrates in place and prevents them from moving with respect to each other. Conductive bump technology is known in the art, and is described, for example, in earlier European Patent Application Publ. No. 444 469 (Art. 54 (3) EPC).

The conductive bumps are preferably formed from indium. One of the advantages of indium is that it has a lower melting temperature than most adhesive bonds and is attacked by acids, so that if access to the secure circuit is attempted by chemical melting through one of the substrates, the electrical connection provided by the indium contacts will be broken. As explained below, this will cause the secure code stored in the memory circuit to be altered, so that even if it is reversed engineered, the wrong code will be discovered.

Solder bumps could be used instead of indium bumps. With solder bumps, however, the spacing between the substrates would be about 25 microns, as opposed to about 4-6 microns for indium bumps. Solder bumps thus leave more clearance between the substrates for inserting a probe to access the secure circuitry. The bumps might also be formed from other conductive materials such as gold or conductive adhesive.

In the preferred embodiment illustrated in the drawings, a power supply circuit for the volatile memory 6a, 6b includes a number of conductive bumps pairs that are connected in series as part of the power supply circuit. Separating or otherwise moving the substrates with respect to each other to gain access to the secure circuitry requires that these pairs be broken. In this event the power supply circuit is interrupted and the volatile memory which it serves changes state, thus rendering harmless any access to the secure circuit after it has been exposed. In the case of a dynamic RAM, the refresh circuit rather than the power supply circuit might be interrupted by moving the substrates relative to each other to implement the memory change of state.

To impede lateral access to the internal circuitry, especially when the substrates are spaced fairly wide apart from each other as in the case of solder bumps, opposed conductive dams 14a and 14b may be formed on substrates 2 and 4, respectively, around the internal circuitry. The conductive

dam 14b on substrate 4 is located in the peripheral region of that substrate, while the conductive 14a dam on substrate 2 is located inward of the contact pads 10. The conductive dams are fabricated in a manner similar to the conductive bumps, and will generally be of the same material. They physically impede lateral access to the internal circuitry, and may be connected in series with the conductive bumps as part of the maintenance circuit. Separating the substrates thus also separates the mating dams, again open circuiting the power supply circuit. The dams on each substrate may be divided into separate segments, with one of the segments included in the power supply circuit and the other segment maintained at a different voltage level. By positioning the segments fairly close to each other, any attempt to probe the internal circuitry through the space between adjacent segments will tend to short circuit the segments, again interrupting the power supply for the secure memory.

While the power supply circuit may make only a single traverse between one substrate and the other, the circuit structure is preferably fabricated so that it makes multiple traverses, thereby providing assurance that it will be interrupted if the structure is tampered with. Such an arrangement is illustrated in FIGs. 1a, 1b and 3. In FIG. 3 the power supply circuit is indicated in dashed lines just below the opposed surfaces of the two substrates, although in practice it would be implemented by a metallization pattern on the surfaces themselves. Also, memory circuits 6a and 6b are shown on the substrate surfaces, while in practice they would be embedded within the substrates.

An external power supply such as a battery is connected to the circuit structure described thus far at one of the contact pads P on substrate 2. An electrical connection is made between contact pad P and one of the conductive bumps A1 on the same substrate by extending under the adjacent dam if present with a dielectric layer separating the two. The circuit continues from bump A1 on substrate 2 to the aligned bump A2 on substrate 4. The convention used for these figures is that, for an aligned pair of conductive bumps or dams, the bump or dam on the power supply side is indicated by the numeral "1", while the opposed bump or dam on the secure circuit side is indicated by the numeral "2". Also, an electrical connection on one substrate is indicated by a solid line, while the image of that connection on the opposed substrate is indicated by a dashed line.

Continuing with the power supply circuit, it extends in succession from bump A2 to bump B1 via lead 16 on substrate 4; from bump B1 to bump B2 on substrate 2; from bump B2 to bump C1 on substrate 2 via lead 18; from bump C1 to bump C2 on substrate 4; from bump C2 to dam D1 via lead 20 on substrate 4; from dam D1 on substrate 4 to dam D2 on substrate 2; from dam D2 to bump E1 via lead 22 on substrate 2; and finally from bump E1 to memory circuit 6a via lead 24 on substrate 2 and to memory 6b via bump E2 and lead 26 on substrate 4. Signal connections between the two segments of the memory circuit are provided along lead 28 (substrate 2) and lead 30 (substrate 4) via bumps F1 and F2.

After assembly, the two substrates may be encapsulated by conventional techniques if desired, with the wire bonding pads around the periphery of substrate 2 left exposed. The completed circuit package 32 can then be mounted to a printed circuit board 34 that includes a power supply such as a battery 36. An opening 38 is formed in the printed circuit board just larger than the outer dimensions of substrate 4, so that the secure circuit package 32 can be mounted to the board with the substrate 4 fitting in opening 38. A series of wire bonding pads 40 on the board around the periphery of opening 38 mate with pads 10 on the larger substrate 2. The battery 36 is connected via lead 42 on the circuit board to a board pad P' that mates with power supply pad P on the substrate 2. The assembly may then be encapsulated within encapsulation layers 44 by conventional techniques, with external contact pads 46 along the periphery of the circuit board 44 left exposed. The assembly may also be packaged separately, independent of an integrated circuit board, using conventional integrated circuit packaging techniques.

While a particular embodiment of the invention has been shown and described, numerous variations and alternate embodiments will occur to those skilled in the art. Accordingly, it is intended that the invention be limited only in terms of the appended claims.

Claims

1. A secure circuit structure, characterized by
   - a pair of opposed substrates (2, 4) with a volatile circuit (6) fabricated on at least one of said substrates (2, 4) and facing the other substrate (4, 2);
   - means (12, A-F) positioning said substrates (2, 4) with respect to each other; and
   - a maintenance circuit (12-26, A-E) for said volatile circuit (6) extending between said substrates (2, 4) such that said maintenance circuit (12-26, A-E) is interrupted, thereby altering said volatile circuit (6), if said substrates (2, 4) are moved with respect to each other.

2. The circuit structure of claim 1, characterized by said maintenance circuit (12-26, A-E) including at least one pair of opposed conductive bumps (12, A-E) extending from said opposed substrates (2, 4) and contacting each other.

3. The circuit structure of claim 2, characterized by said bumps (12, A-E) comprising at least a portion of said positioning means (12, A-F).

4. The circuit structure of claims 2 or 3, characterized by said bumps (12, A-E) being formed from indium.

5. The circuit structure of any of claims 2 - 4, characterized by said maintenance circuit (12-26, A-E) extending in multiple traverses back and forth between said substrates (2, 4) through said bumps (12, A-E) such that, if said substrates (2, 4) are moved with respect to each other, the electrical connectivity of said maintenance circuit (12-26, A-E) is altered via open circuiting the maintenance circuit (12-26, A-E), interrupting the supply of maintenance signals which maintain the secure contents of said volatile circuitry (6).

6. The circuit structure of any of claims 2 - 5, characterized by said bumps (12, A-E) being located inward from the peripheries of said substrates (2, 4) said maintenance circuit (12-26, A-E) further including at least one pair of opposed conductive dams (14, D) extending from said opposed substrates (2, 4) in the peripheral region of at least one of the substrates (2, 4) and contacting each other, said dams (14, D) impeding access to the interior of said circuit structure (32).

7. The circuit structure of claim 6, characterized by multiple pairs (14a, 14b, D1, D2) of said dams (14, D) that are segmented with respect to each other, said dams (14, D) being connected in said maintenance circuit (12-26, A-E) such that open circuiting a pair (14a, 14b, D1, D2) of opposed dams (14, D) by moving said substrates (2, 4) with respect to each other or short circuiting adjacent segmented dams (14, D) by attempting to probe between them alters the electrical connectivity of said maintenance circuit (12-26, A-E), thus interrupting the supply of maintenance signals which maintain the secure contents of said volatile circuitry (6).

8. The circuit structure of claim 1, characterized in that said volatile circuit (6) is divided into portions (6a, 6b) located on each of said substrates (2, 4), said maintenance circuit (12-26, A-E) interconnecting the portions (6a, 6b) of said volatile circuit (6) on each substrate (2, 4).

9. The circuit structure of any of claims 1 - 8, characterized by a larger circuit on at least one of said substrates (2, 4), said volatile circuit comprising a portion of said larger circuit.

10. The circuit structure of any of claims 1 - 9, characterized by said maintenance circuit (12-26, A-E) comprising a power supply circuit for said volatile circuit (6).

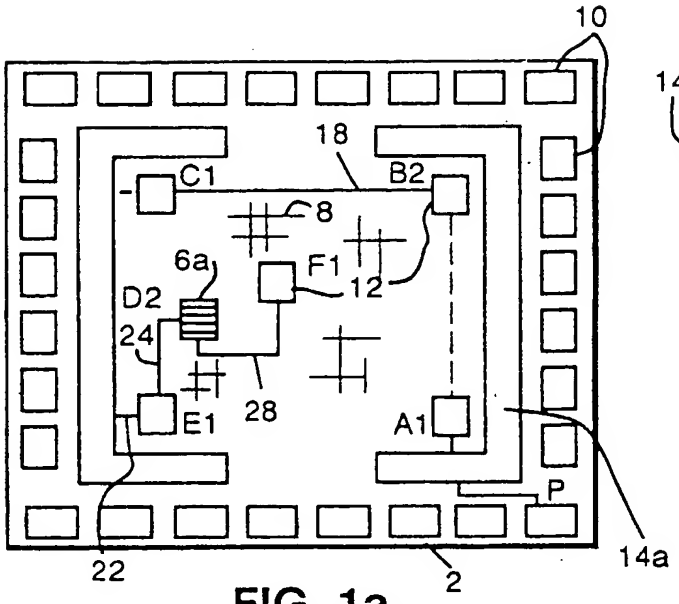

FIG. 1a.

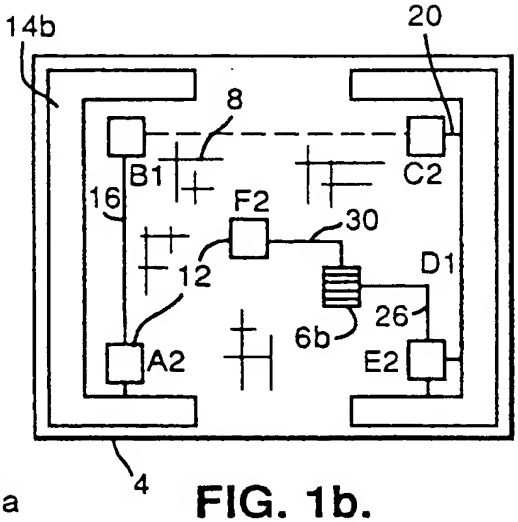

FIG. 1b.

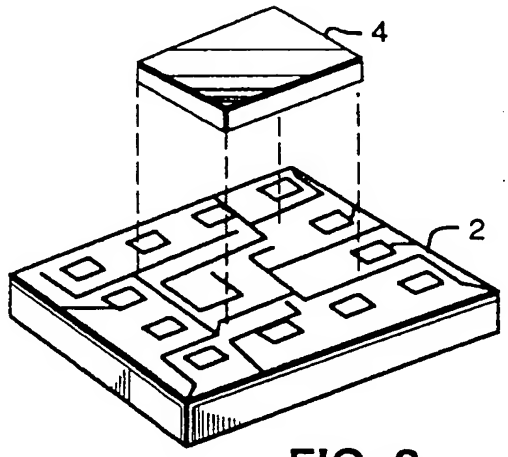

FIG. 2.

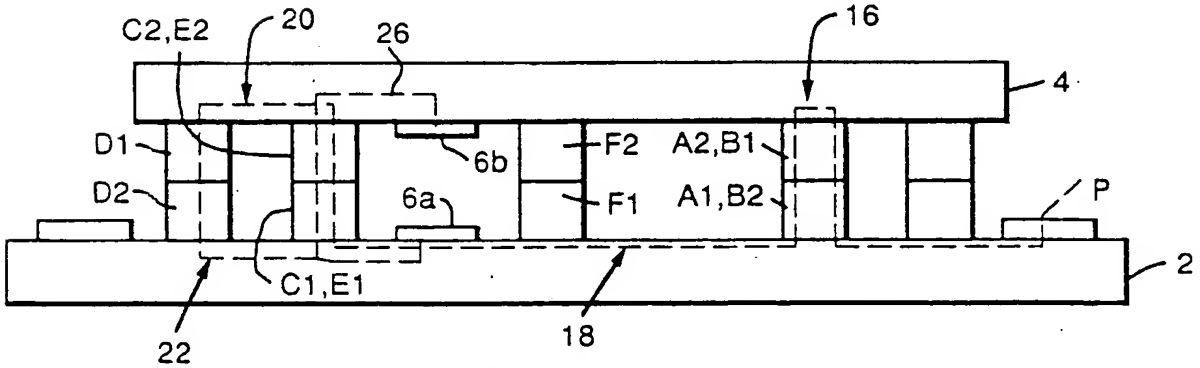

FIG. 3.

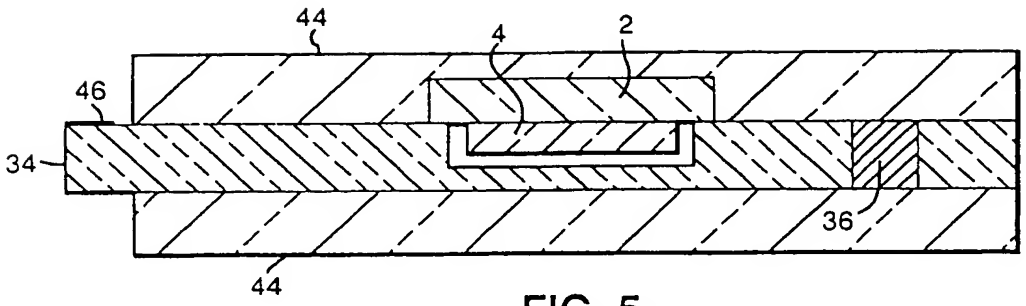

FIG. 5.

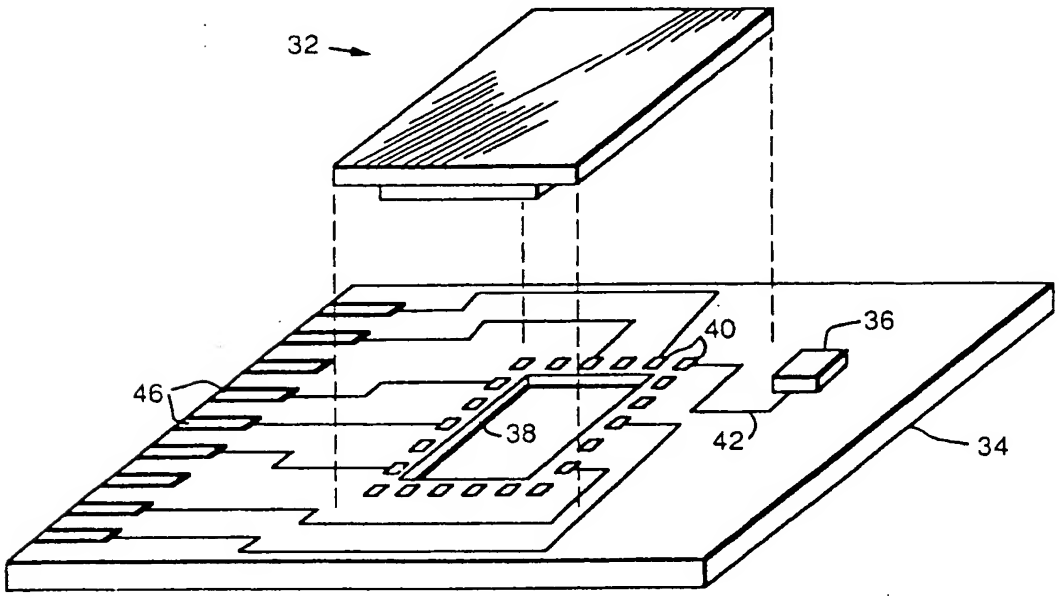

FIG. 4.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 510 433 A3**

(12) EUROPEAN PATENT APPLICATION

(21) Application number: 92106105.7

(22) Date of filing: 09.04.92

(51) Int. Cl.5: **H01L 25/18**, H01L 23/58, G11C 7/00

(30) Priority: 26.04.91 US 692334

(43) Date of publication of application:
28.10.92 Bulletin 92/44

(84) Designated Contracting States:
FR GB

(88) Date of deferred publication of the search report:
25.08.93 Bulletin 93/34

(71) Applicant: Hughes Aircraft Company
7200 Hughes Terrace P.O. Box 45066
Los Angeles, California 90045-0066(US)

(72) Inventor: Thiele, Alan G.
3444 Lady Hill Road
San Diego, California 92130(US)
Inventor: Williams, Ronald L.
1421 Pine Heights Way
San Marcos, California 92069(US)

(74) Representative: Witte, Alexander, Dr.-Ing. et al
Witte, Weller, Gahlert & Otten Patentanwälte
Augustenstrasse 14
D-70178 Stuttgart (DE)

(54) Secure circuit structure.

(57) A secure circuit structure includes a pair of opposed substrates (2, 4) having a volatile circuit (6a, 6b) fabricated on at least one, and perferably both substrates (2, 4). A maintenance circuit (12-26, A-E) for the volatile circuit (6a, 6b) extends between the substrates (2, 4) so that it is interrupted, thereby altering the volatile circuit (6a, 6b) and rendering reverse engineering attempts futile, if the substrates (2, 4) are moved with respect to each other by opening the circuit package. The maintenance circuit (12-26, A-E) preferably includes a series of mating conductive indium bumps (12, 14, A-E) that extend from the opposed substrates (2, 4) and mechanically bond the substrates (2, 4) together. The secured volatile circuit (6a, 6b) may be a random access memory storing an access code, maintained by a battery power supply circuit.

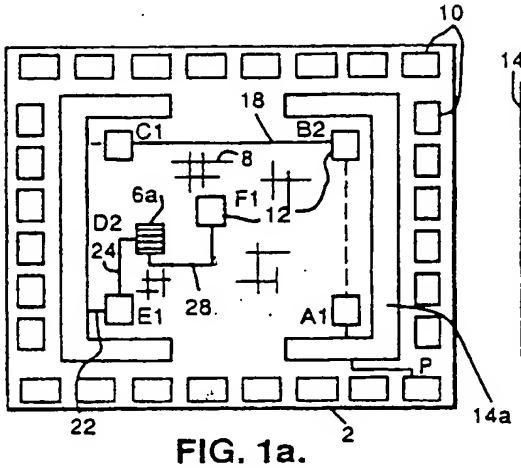

FIG. 1a.

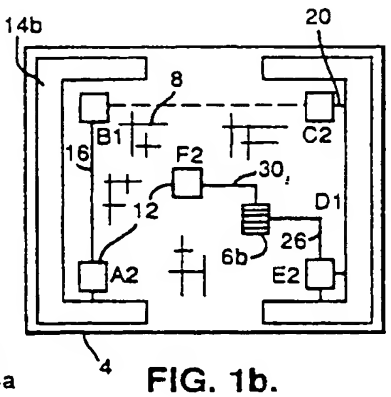

FIG. 1b.

EP 0 510 433 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 92 10 6105

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
X	IBM TECHNICAL DISCLOSURE BULLETIN. vol. 32, no. 1, June 1989, NEW YORK US pages 46 - 49 'Partitioning function and packaging of integrated circuits for physical security of data'	1,2,5,8	H01L25/18 H01L23/58 G11C7/00
Y	* page 48, line 20 - page 49, line 5; figure *	3,4,6,10	
A		9	

Y	WO-A-8 902 653 (IRVINE SENSORS CORPORATION)	3,4	
A	* page 1, line 4 - line 34 * * page 4, line 10 - page 5, line 30; figures 1,2 * * page 10, line 29 - page 11, line 29; figures 7-10 *	1,2	

Y	GB-A-2 195 478 (NCR CORPORATION)	10	
A	* page 2, left column, line 38 - right column, line 92; figures 1,2 * * page 3, right column, line 82 - page 5, right column, line 76; figures 8-11 *	1,5-7	
	---		TECHNICAL FIELDS SEARCHED (Int. Cl.5)
Y	DE-A-3 002 740 (HITACHI LTD) * page 10, line 10 - page 11, line 19; figures 2,3 *	6	G11C G06F H01L

P,D, A	EP-A-0 444 469 (HUGHES AIRCRAFT CO.) * column 2, line 32 - column 4, line 1; figures 1-4 *	1-3	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	24 JUNE 1993	CUMMINGS A.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P0401)

DOCKET NO: 1999P1778
SERIAL NO:
APPLICANT: Andreas Kux et al.

LERNER AND GREENBERG P.A.
P.O. BOX 2480
HOLLYWOOD, FLORIDA 33022
TEL. (954) 925-1100